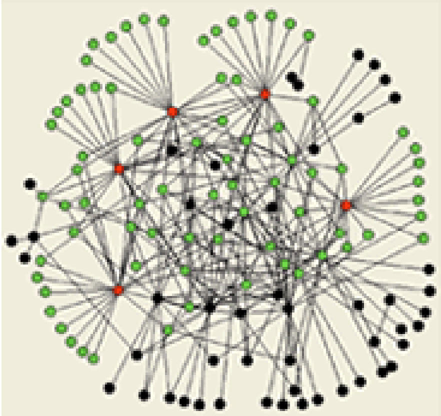
Threat Networks and Threatened Networks:

Basic Principles and Practical Applications

L.A. Braunstein / S.V. Buldyrev / Y. Chen / R. Cohen / S. Havlin / T. Kalisky / G. Li / E. Lopez / G. Paul / S. Sreenivasan / H. E. Stanley / T. Tanizawa / Z. Wu



Acknowledgements:

- 2002 ONR Wash (Malecki, Goolsby, Shlesinger)
- 2003 ONR-DURIP: >> 10^6 network nodes
- 2003 ONR-IFO NICOP: Prof. Shlomo Havlin
- 2004 ONR-GLOBAL STEP: Prof. Lidia Braunstein
- 2004 National Academy of Sciences
- 2004 IUPAP Boltzmann Medal
- 2005 Physical Review Letters, Nature, PNAS,…

ONR-DURIP Computer Cluster

- 62 AMD Opteron processors
  - 26 2GB dual processor nodes
  - 5 8GB dual processor nodes
- 92 GB total memory
- Specialized network software package ("LEDA")

Threat Networks and Threatened Networks: Basic Principles and Practical Applications

Q1: What are the problems?

- Basic research in the science of network analysis to improve military and intelligence approaches for attacking and defending warfighting networks
- Development of improved tools for analysis of critical warfighting networks and for the disruption of opposing networks

Q2: Why care?

- Scientific: New Laws of Threat and Threatened Networks
- Practical: Random attack vs. Targeted attack

Q3: What do “we” do?

“We”: L.A. Braunstein / S.V. Buldyrev / Y. Chen / R. Cohen / S. Havlin /
T. Kalisky / G. Li / E. Lopez / G. Paul / S. Sreenivasan /
H. E. Stanley / T. Tanizawa / Z. Wu

Outline

1. *Background*
2. *Network Immunization Strategies*
3. *Designing Networks Resilient Against Attack*
    - A. *Network Integrity: A Network Design Tool (NetOpt)*
    - B. *Network Efficiency*
    - C. *Network Flow*
4. *Designing Optimal Attack Tool (NetAttack)*
5. *Future work*

TWO TAKE HOME MSGS:

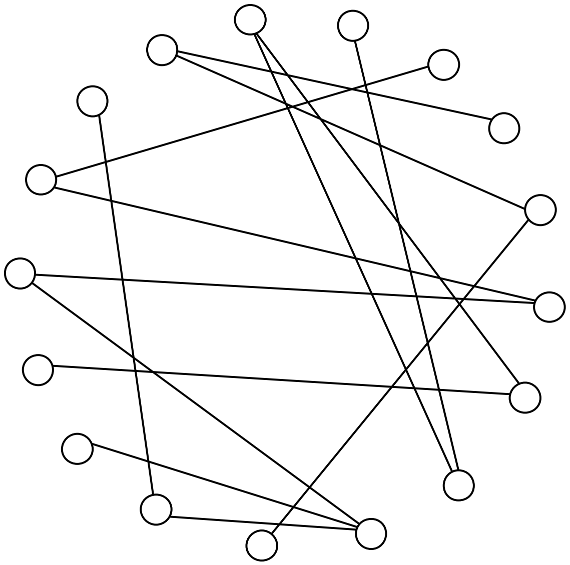
Statistical physics concepts are useful to

- Determine optimal network designs against real-world attack scenarios.
- Determine optimal attack strategies against specific terrorist networks.

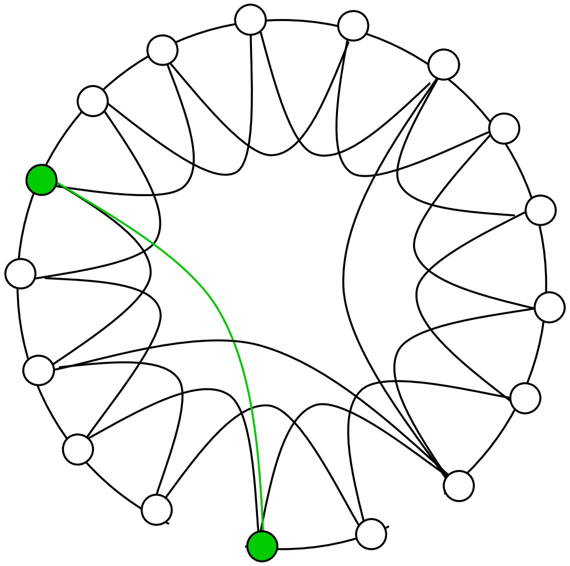
1. Background

3 families of networks:

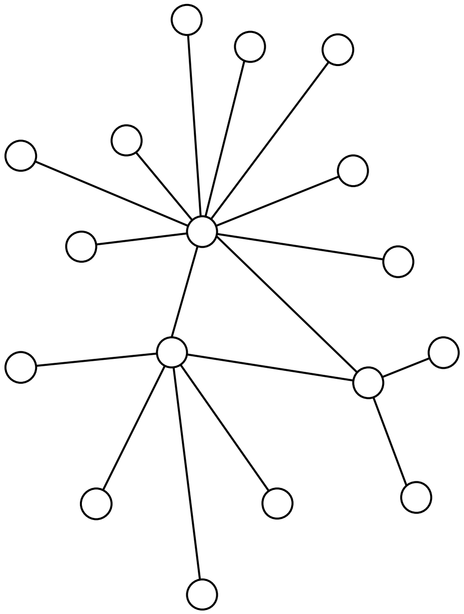
Erdös-Rényi
(Exponential tail)



Watts-Strogatz



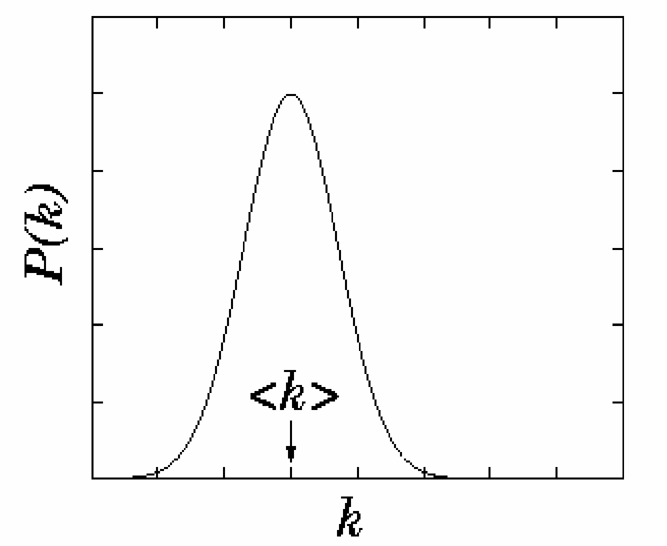
Scale-free
(Power law tail)



Real world examples of scale-free networks:
(1) Airline route map (Note: Hubs)

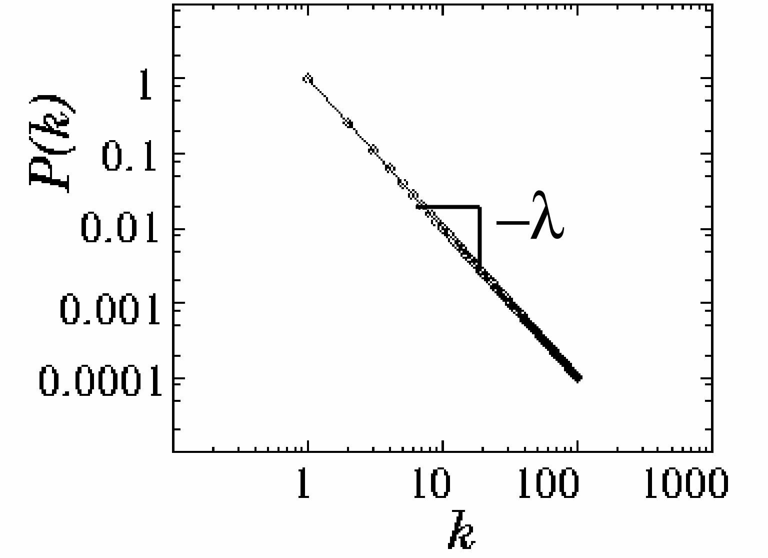
Histograms: Number of nodes of degree *k*

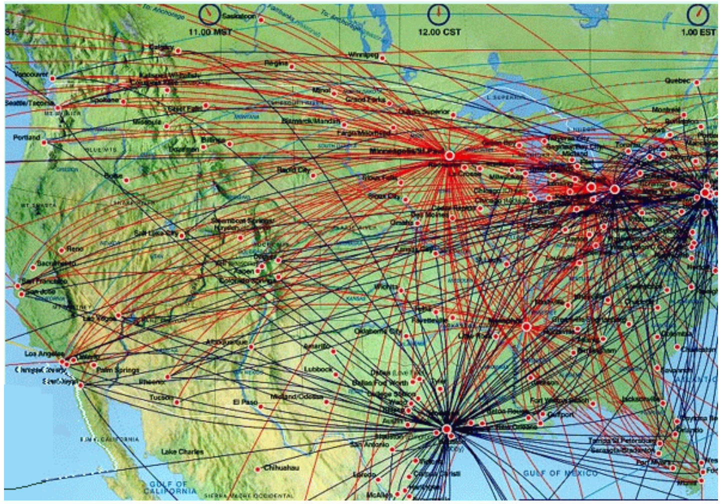
Poisson distribution (exponential tail)



Exponential Tail

Scale-free distribution (power law tail)

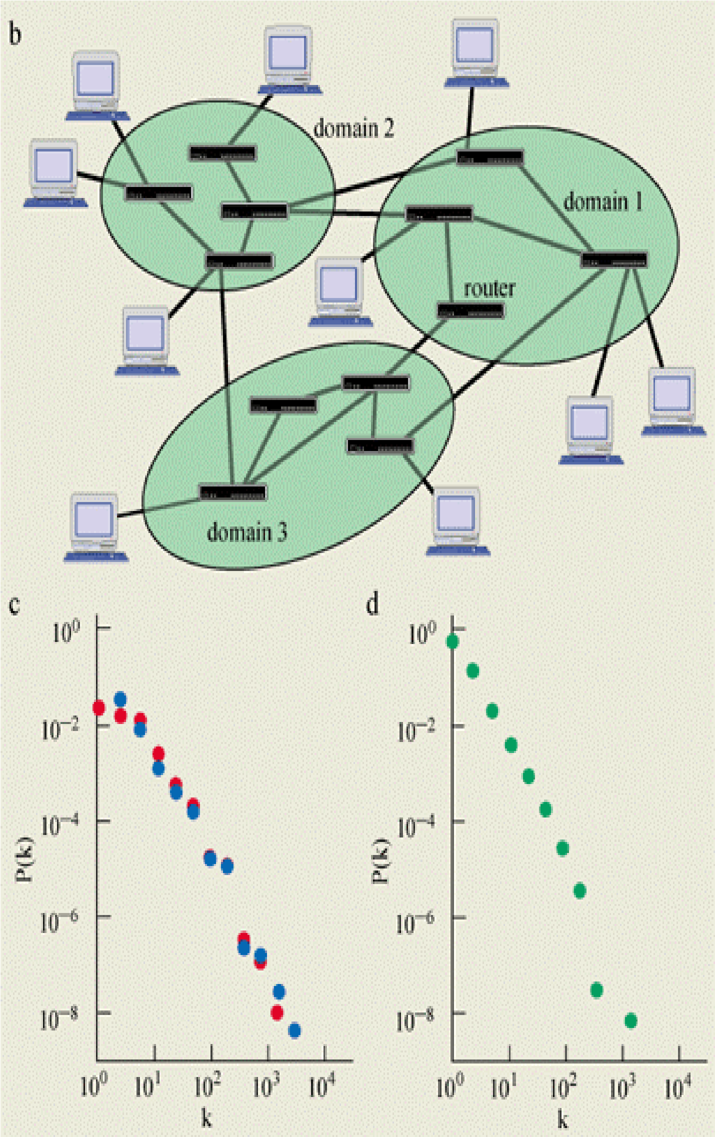


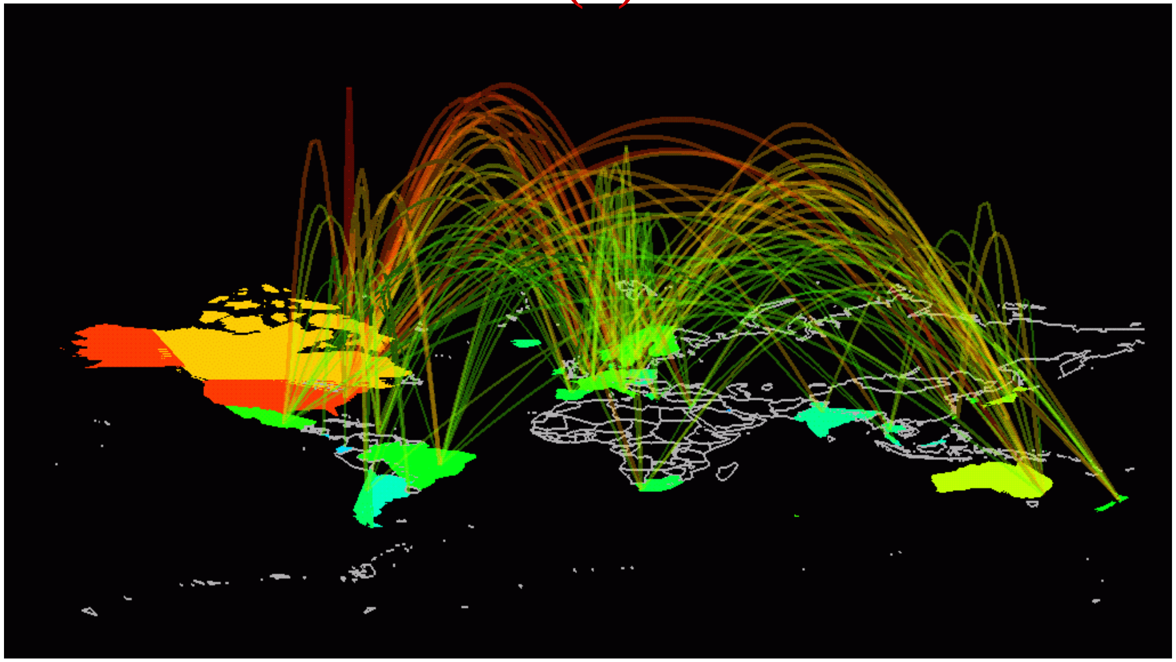


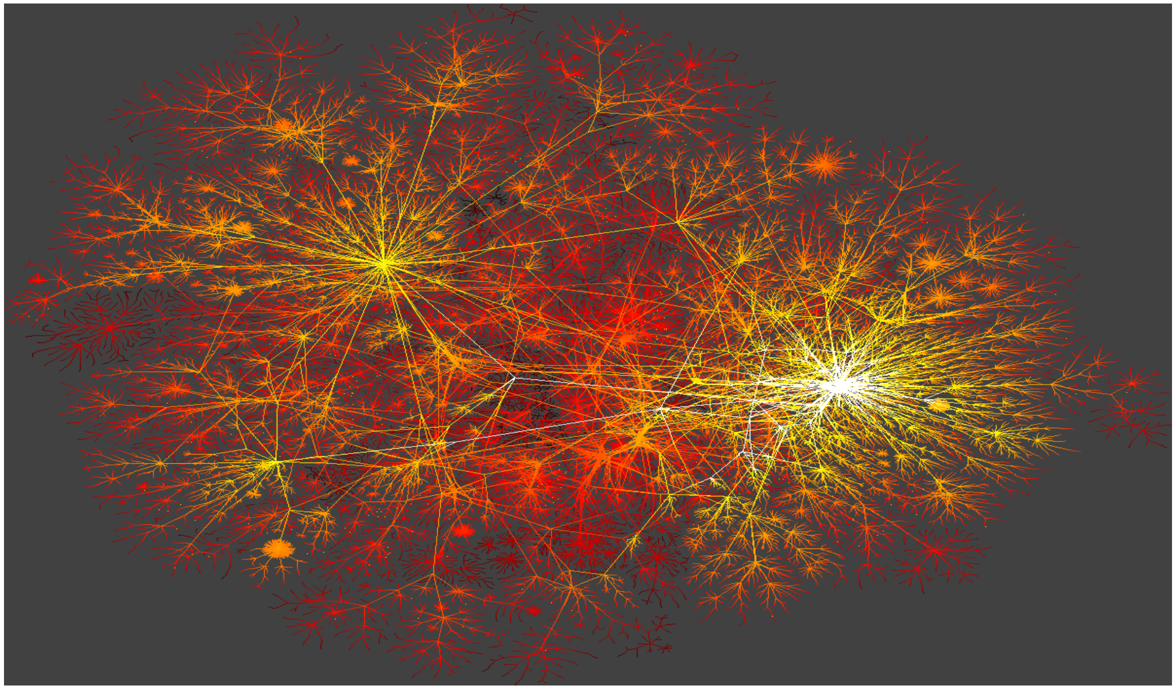
Power Law Tail

Real world example of scale-free networks: (2) Internet Network

Faloutsos et. al., SIGCOMM ’99



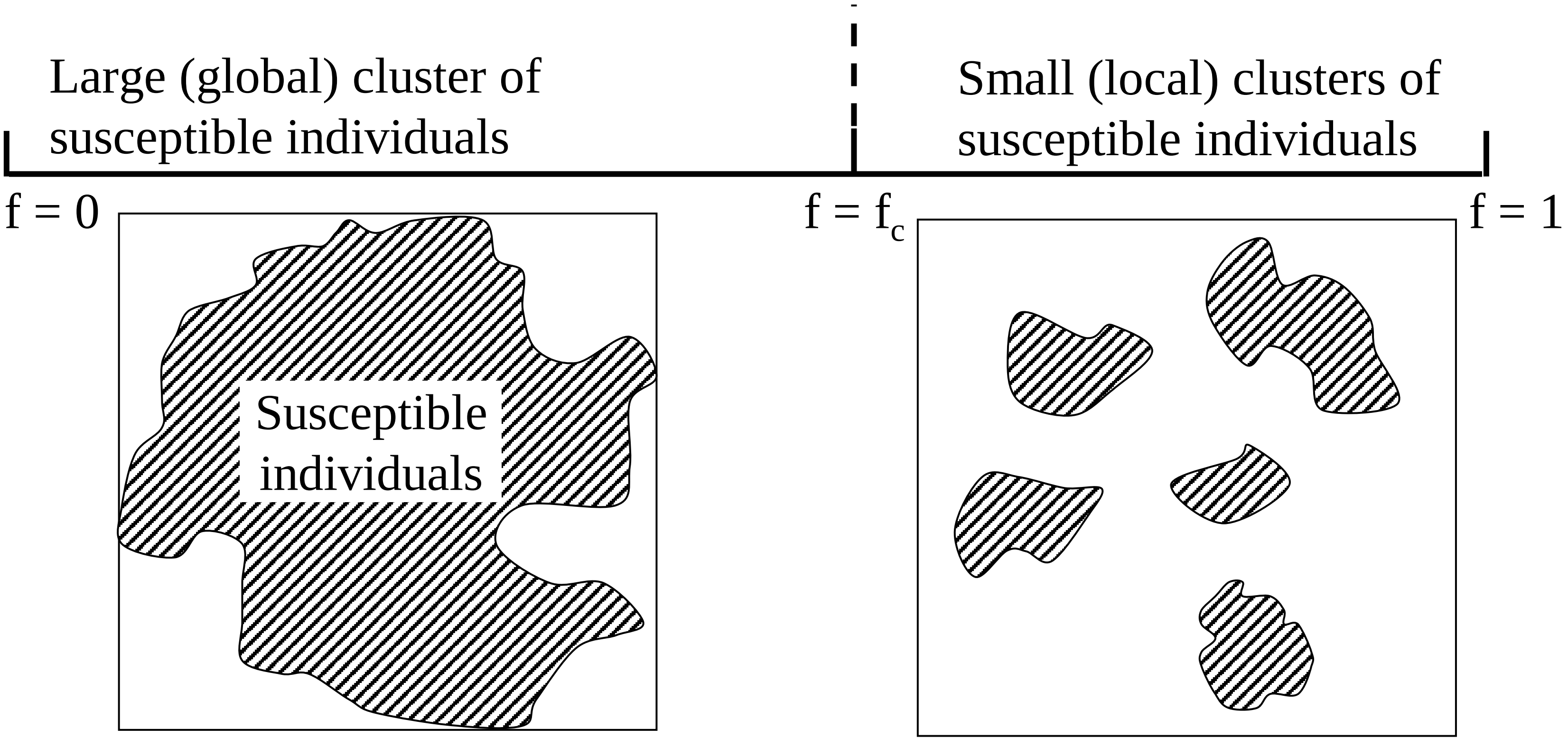




2. Network Immunization Strategies

Goal of efficient immunization strategy:

- Immunize at least a critical fraction f_c (“Immunization threshold”) of the number of individuals so that only isolated clusters of susceptible individuals remain.
- Effective without detailed knowledge of the network.



Large (global) cluster of susceptible individuals

Small (local) clusters of susceptible individuals

$f = 0$

$f = f_c$

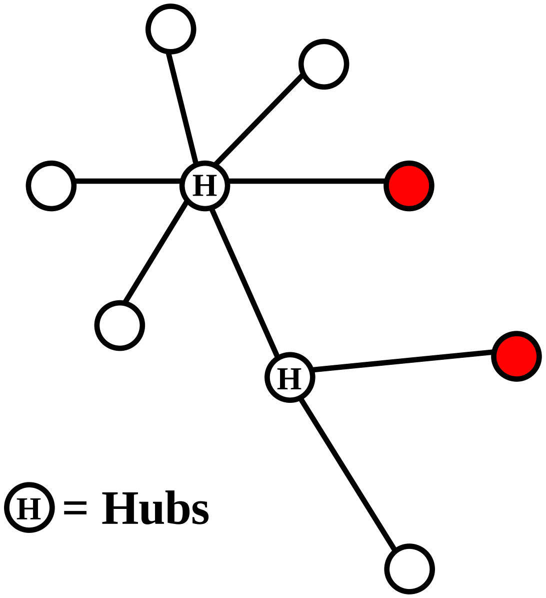
$f = 1$

Three immunization strategies

Ex: Immunize 2 of the 9 nodes

Random:

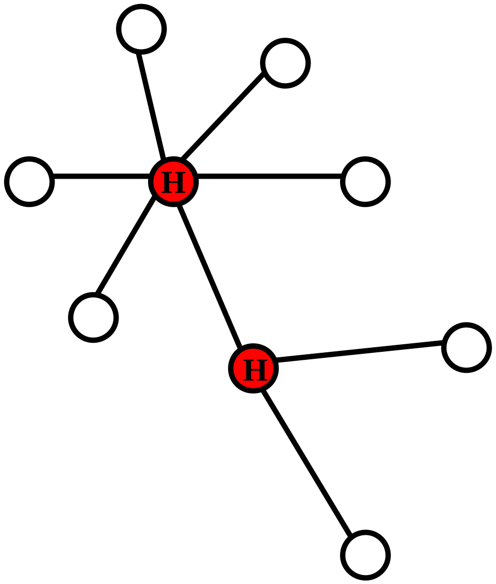
2/9



- **High immunization threshold**
- **No prior network information needed**

Targeted:

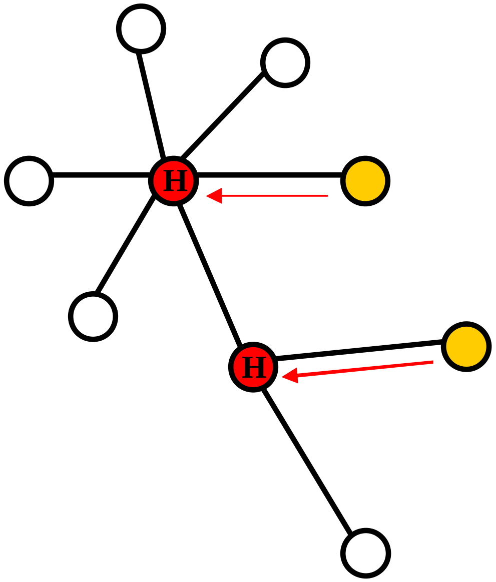
1



- **Low immunization threshold**
- **Knowledge of hubs (highly connected individuals) needed**

Acquaintance:

7/9

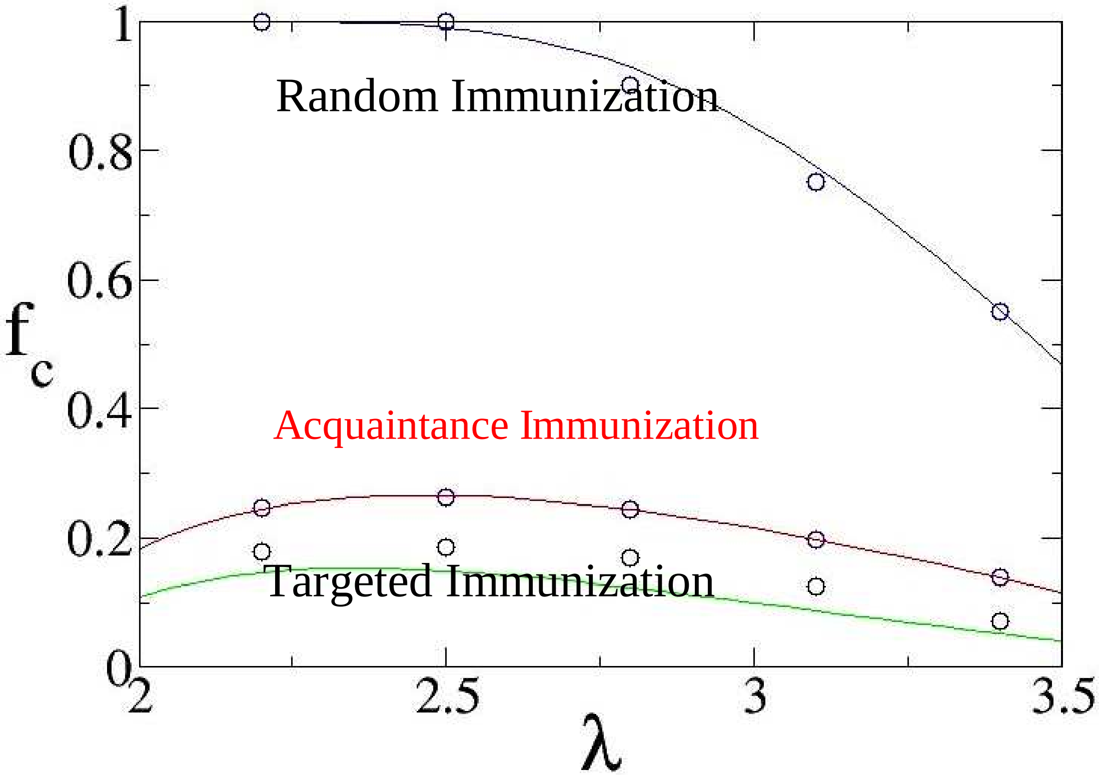


- **Low immunization threshold**
- **No prior network information needed**

Effectiveness of Immunization Strategies

Goal: Minimize f_c

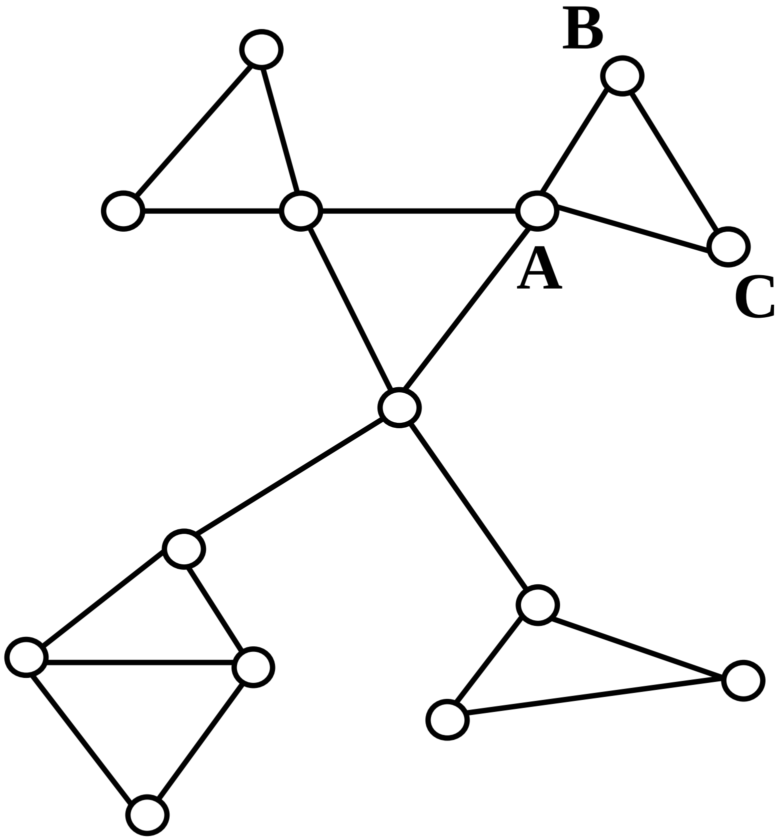
Immunization threshold f_c (scale-free case)



Cohen, Havlin, Ben-Avraham Phy. Rev. Lett (2003)

THM: Acquaintance Immunization is more efficient than Random Immunization.

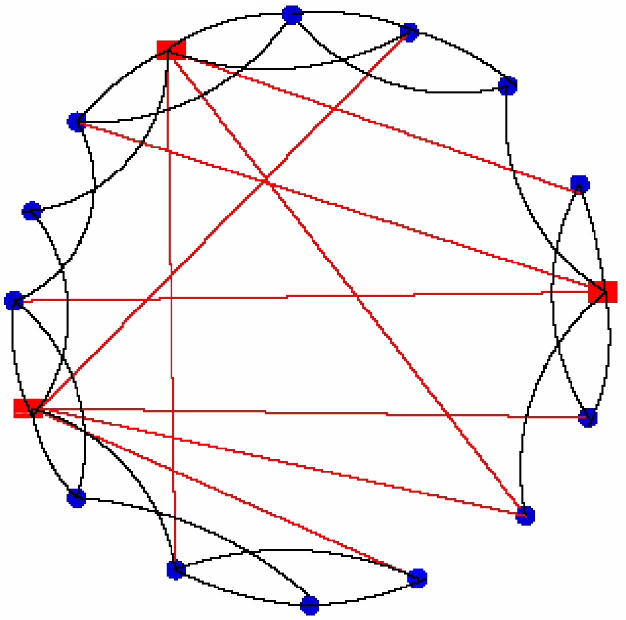
Clustering: “My friends are also friends”



- **Clustering is quantified by the clustering coefficient.**
- **Social networks have high clustering coefficient.**

Immunization of social networks

Characteristic features of social networks



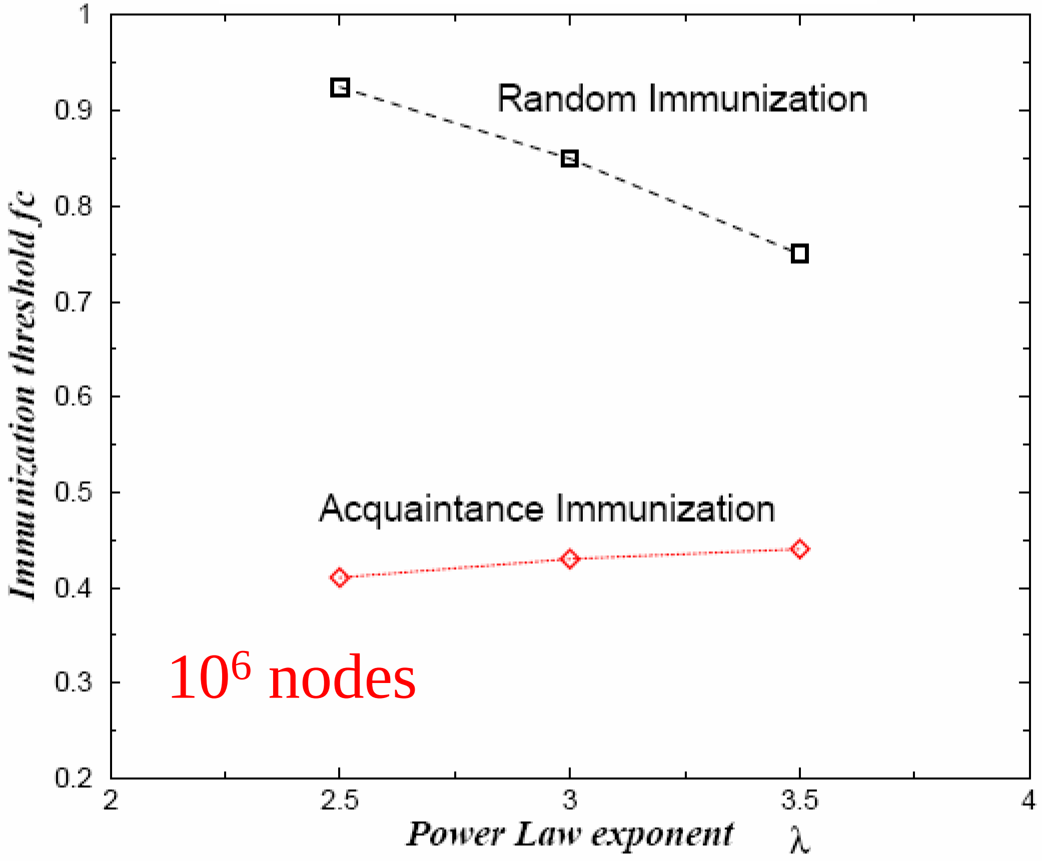
- Power-law degree distribution
- “six degrees of separation” property
- High geographical clustering

We test the acquaintance immunization strategy on a social network model which incorporates the above features.

Acquaintance immunization is effective in social networks

(since f_c lower for acquaintance immunization than for random immunization)

Clustering Coefficient = 0.37

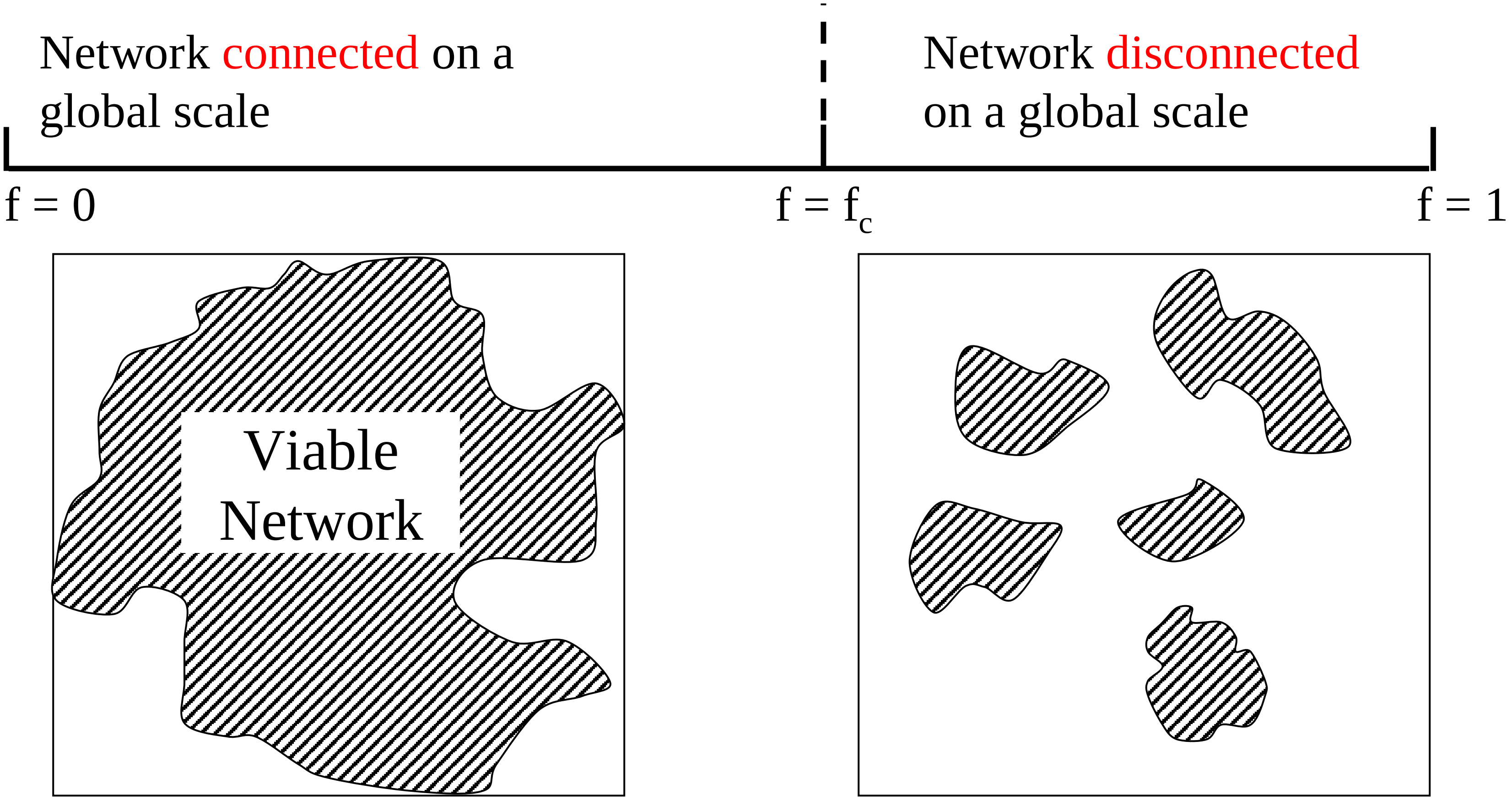


10^6 nodes

3. Designing networks resilient against attack

Immunization Goal: Destroy connectivity (low threshold f_c)

Resilience Goal: Preserve connectivity (high threshold f_c)



Network connected on a global scale

Network disconnected on a global scale

$f = 0$

$f = f_c$

$f = 1$

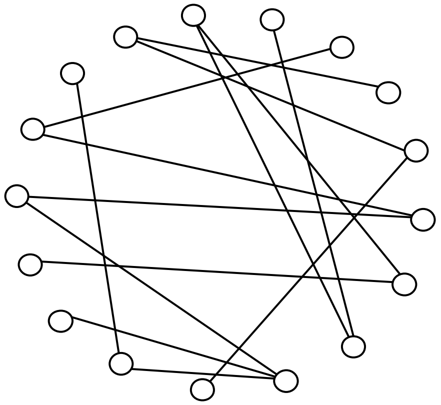
3A. Network Integrity:

Realistic model

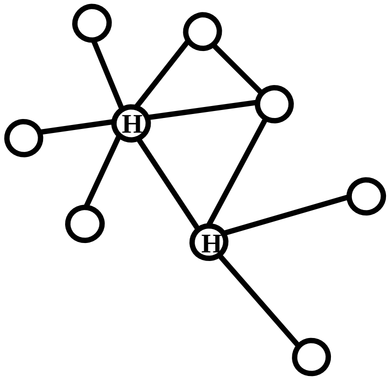
Multiple waves of alternating

- Random failures (attacks probability p_r)
- Targeted attack (attack probability p_t)

Erdös-Rényi



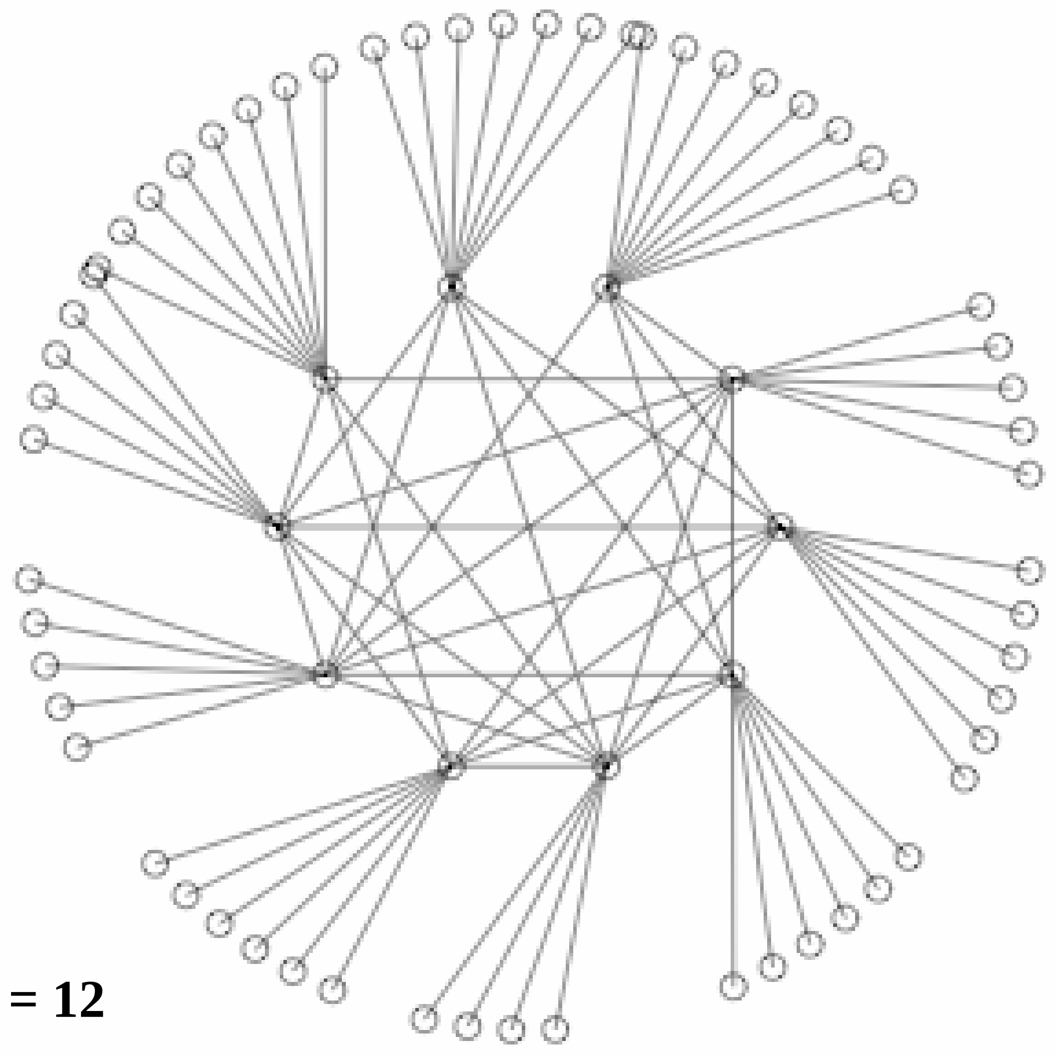
scale-free



- Random attack:
  must remove ≈ 50% to destroy
- Targeted attack:
  must remove ≈ 50% to destroy

- Random attack:
  must remove ≈ 99% to destroy
- Targeted attack:
  must remove ≈ 1% to destroy

Maximally Resilient Network: Example



Given: N = 100,

$\langle k \rangle = 2.1$,

$p_t / p_r = 0.05$

Optimal design is:

$r = 2 * 0.05 = 0.1$

90 nodes of degree:

$k_1=1$

10 "hubs" of degree:

$k_2 = (<k> - 1 + r) / r$

$= (2.1 - 1 + 0.1) / 0.1 = 12$

Networks with Maximum Resilience

Simultaneous waves of targeted and random attacks

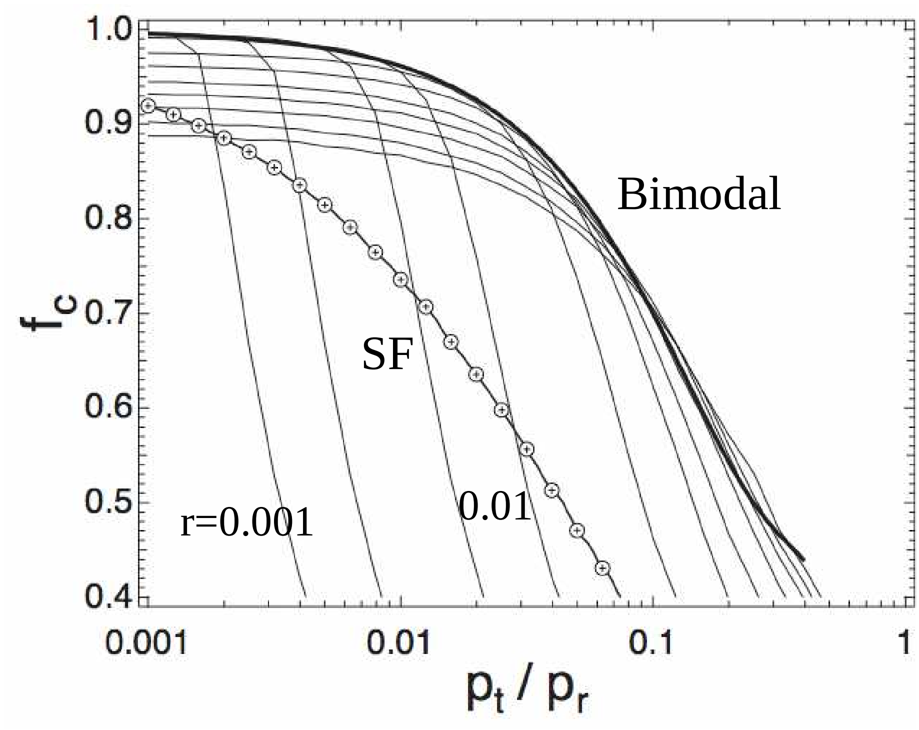
Bimodal: fraction (1– r) having k_1 =1 links and r having k_2 =(<k> − 1+r) / r links.

r = 0.001 — 0.15 from left to right

Optimal Bimodal : $r \cong 2(p_t / p_r)$

p_r - Fraction of nodes removed in a random attack

p_t - Fraction of nodes removed in a targeted attack

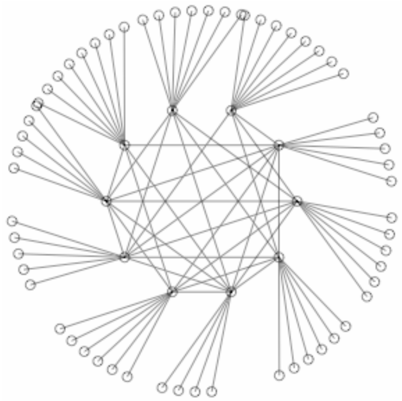


Paul et al. Europhys. J. B 38, 187 (2004), (cond-mat/0404331)

Tanizawa et al. Optimization of Network Robustness to Waves of Targeted and Random Attacks, PRE in press

Our findings

- Our maximally resilient network is more resilient than strictly Erdös-Rényi or scale-free networks to waves of attacks. (Surprisingly, our maximally resilient network has no scale-free attributes)
- Maximally resilient network has bimodal degree distribution
  - Fraction 1 – r of nodes have degree $k_1 = 1$
  - Fraction $r \approx 2\, p_t / p_r$ of nodes have higher degree: $k_2 = (\langle k \rangle - 1 + r) / r$



3A. Optimal Network Design Tool: NetOpt

Protecting Threatened Networks

Motivation: Accessible tool for designing optimal threatened networks

- Input:
  - Size of network
  - Cost goal (number of links)
  - Type of (node) attack
    - Random
    - Targeted
    - Combination
- Output: optimal design for each type of attack

  Optimal solutions are uni- or bi- modal (currently extending to multilevel networks)

NetOpt Software Program

- Encapsulates fast algorithms from our published results
- Generates a specific network from family of optimized networks
- Generates very large optimal networks very quickly – no need for long simulations

* * * * * *

Interactive Demo of Current Version

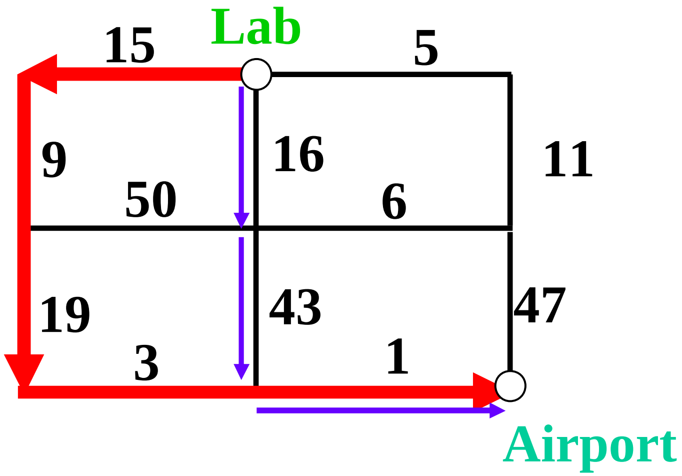
3B. Network Efficiency

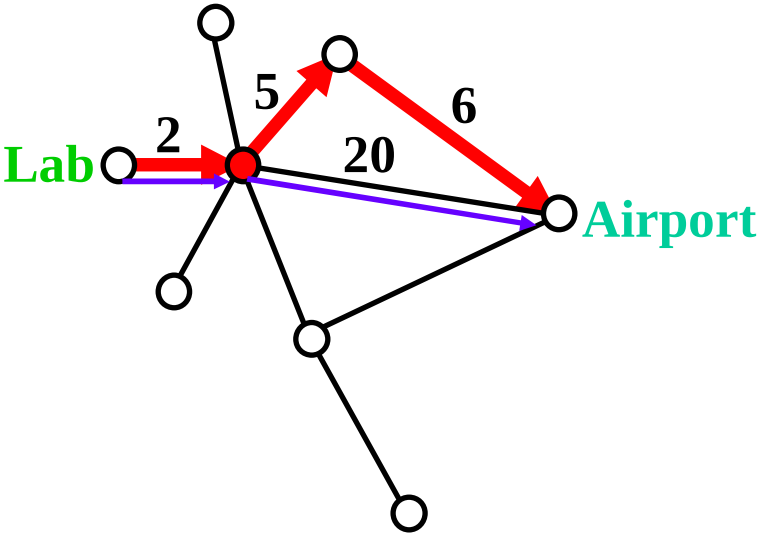
- Before: focus on protecting network integrity against attack (connectivity maintained)

- Now: focus on protecting network efficiency against attack (optimal path maintained)

1. L.A. Braunstein, S.V. Buldyrev, R. Cohen, S. Havlin and H. E. Stanley Phys. Rev. Lett. (2003)
2. S. Sreenivasan, T. Kalisky, L.A. Braunstein, S.V. Buldyrev, S. Havlin and H. E. Stanley, Phys. Rev. E (2004)

Optimal Path: Minimize total "cost"





For this example:

Shortest path: 3 (cost = 60)

Optimal path: 5 (cost = 47)

Shortest path: 2 (cost = 22)

Optimal path: 3 (cost = 13)

Generally:

Shortest path = $N^{0.50}$

Optimal path = $N^{0.61}$

$N^{0.50} < N^{0.61}$

ex: $(10^6)^{0.50} < (10^6)^{0.61}$

Shortest path = Log N

Optimal path = $N^{1/3}$

$\text{Log } N \ll N^{1/3}$

ex: $N=10^6$, $\log 10^6 \ll (10^6)^{1/3}$

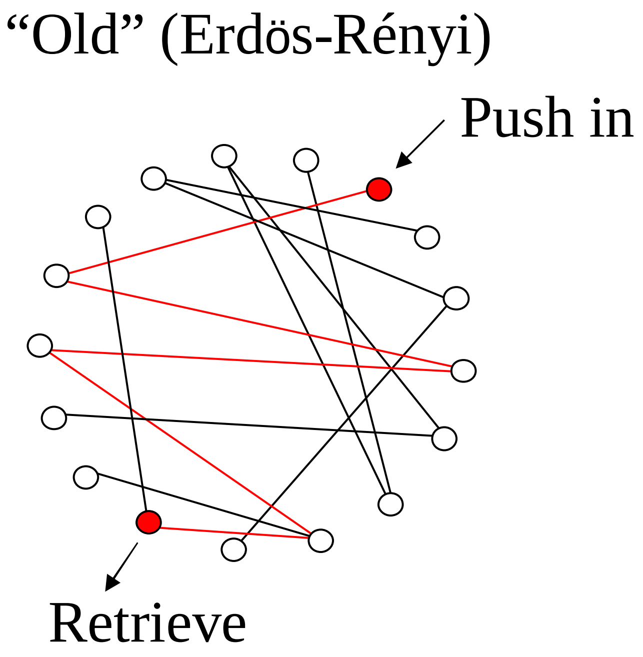
3C. Network Flow

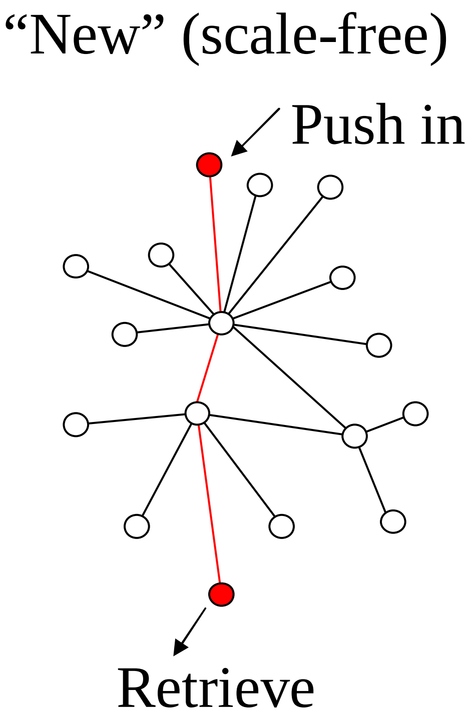
- Before: focus on protecting network integrity and efficiency.
- Now: focus on maximizing network flow (network structure which gives the highest flow).

1. E. Lopez, S.V. Buldyrev, S. Havlin and H. E. Stanley, preprint (2005)
2. Z. Wu, E. Lopez, S. V. Buldyrev, L. A. Brauntein, S. Havlin and H. E. Stanley, PRE in press, 2005

What is network flow?

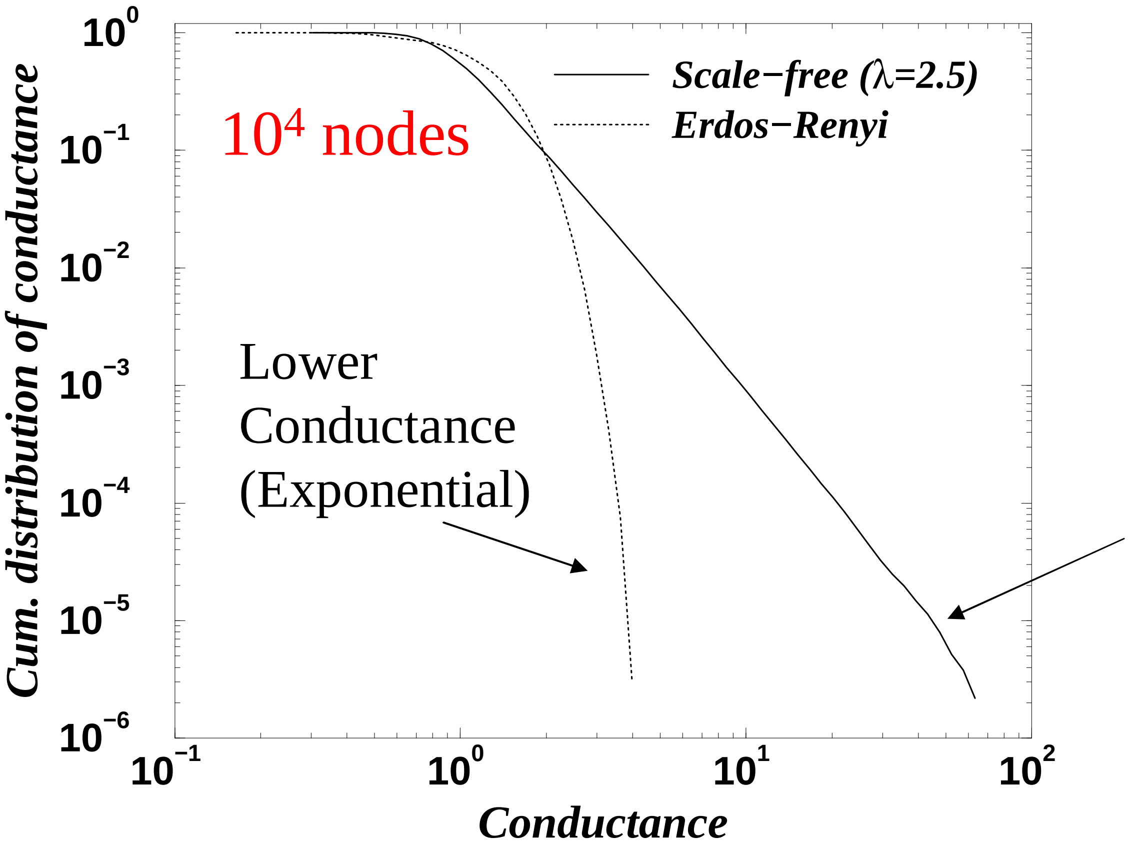
- “Push” into a network goods, electrical current, cars, information etc.
- Higher flow means higher flow of goods, etc., given same “push”.





Scale-free networks have higher flow

(Due to hub spoke structure)



10^4 nodes

Lower
Conductance
(Exponential)

Higher
Conductance
(Power law)

4. Network Attack Tool: NetAttack

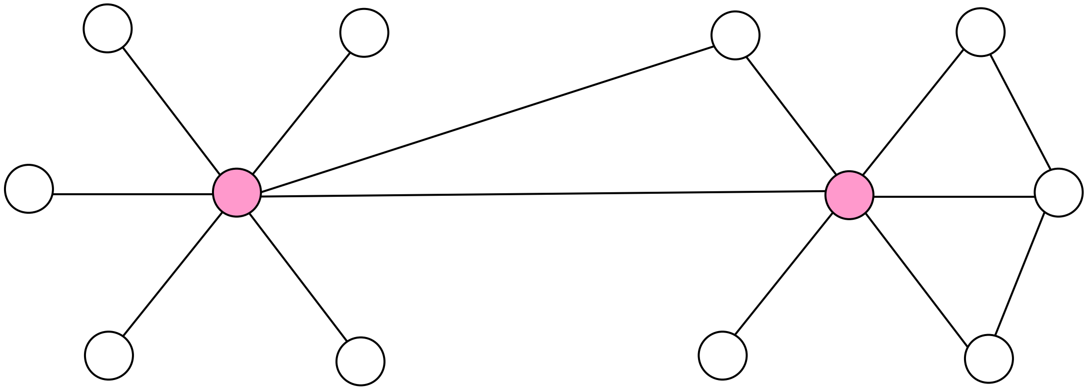
Attacking Threat Networks

- Given a terrorist network, identify critical links/nodes, which must be removed in order to cause maximum network damage.
- Nodes can be weighted by importance.
- Method of identification based on
  - Optimal Path/Centrality
  - Flow

Remove most-central/highest-flow nodes/links from network

Network Attack Tool

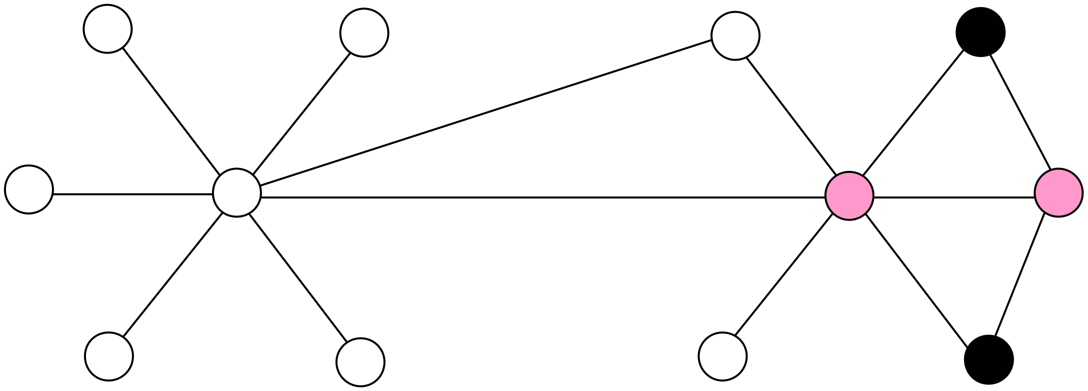
- Example 1- Unweighted nodes



🔴 Nodes to attack

● Most important nodes

- Example 2 - Weighted nodes



5. Future Work

- Improve Network Design Tool
- Implement Network Attack Tool
- Network efficiency and flow as quantities to be optimized
- Other real world network attributes/constraints
- 6 x 10^9 node networks (needed for reliable predictions)

Summary

Statistical physics concepts can indeed be used to

- Determine optimal network designs against real-world attack scenarios.
- Determine optimal attack strategies against specific terrorist networks.

Acknowledgements

- ONR Washington (Goolsby)
- 2003 ONR DURIP: > 10^6 network nodes
- 2003 ONR-IFO NICOP: Prof. Shlomo Havlin
- 2004 ONR-GLOBAL STEP: Prof. Lidia Braunstein
- 2003 Physical Review Letters
- 2004 National Academy of Sciences
- 2004 IUPAP Boltzmann Medal